EXHIBIT 5

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

UMBRA Technologies Ltd. ("UMBRA") provides evidence of infringement of claims 1-9 of U.S. Patent No. 10,574,482 (hereinafter "the '482 patent") by VMware Inc. ("VMware"). In support thereof, UMBRA provides the following claim charts.

"Accused Instrumentalities" as used herein refers to at least VMware systems and methods, including one or more hardware and software products for network virtualization and related services, which by way of example include but are not limited to VMware SD-WAN, (*see, e.g.*, VMware SD-WAN, https://www.vmware.com/products/sd-wan.html), VMware NSX software-defined data center (*see, e.g.*, VMware NSX, https://www.vmware.com/products/nsx.html), VMware vSphere (*see, e.g.*, VMware vSphere, https://www.vmware.com/products/vsphere.html), and VMware Horizon (*see, e.g.*, VMware Horizon, https://www.vmware.com/products/horizon.html) and related earlier versions (the "Accused Instrumentalities"). These claim charts demonstrate VMware's infringement, and provide notice of such infringement, by comparing each element of the asserted claims to corresponding components, aspects, and/or features of the Accused Instrumentalities. These claim charts are not intended to constitute an expert report on infringement. These claim charts include information provided by way of example, and not by way of limitation.

The analysis set forth below is based only upon information from publicly available resources regarding the Accused Instrumentalities, as VMware has not yet provided any non-public information. An analysis of VMware's (or other third parties') technical documentation and/or software source code may assist in fully identifying all infringing features and functionality. Accordingly, UMBRA reserves the right to supplement this infringement analysis once such information is made available to UMBRA. Furthermore, UMBRA reserves the right to revise this infringement analysis, as appropriate, upon issuance of a court order construing any terms recited in the asserted claims. UMBRA provides this evidence of infringement and related analysis without the benefit of claim construction or expert reports or discovery. UMBRA reserves the right to supplement, amend or otherwise modify this analysis and/or evidence based on any such claim construction or expert reports or discovery.

Note: All internet sources last accessed and downloaded July 31, 2023.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

Unless otherwise noted, UMBRA contends that VMware directly infringes the '482 patent in violation of 35 U.S.C. § 271(a) by selling, offering to sell, making, using, and/or importing the Accused Instrumentalities. The following exemplary analysis demonstrates that infringement. Unless otherwise noted, UMBRA further contends that the evidence below supports a finding of indirect infringement under 35 U.S.C. §§ 271(b) and/or (c), in conjunction with other evidence of liability under one or more of those subsections. VMware makes, uses, sells, imports, or offers for sale in the United States, or has made, used, sold, imported, or offered for sale in the past, without authority, or induces others to make, use, sell, import, or offer for sale in the United States, or has induced others to make, use, sell, import, or offer for sale in the past, without authority products, equipment, or services that infringe claims 1-9 of the '482 patent, including without limitation, the Accused Instrumentalities.

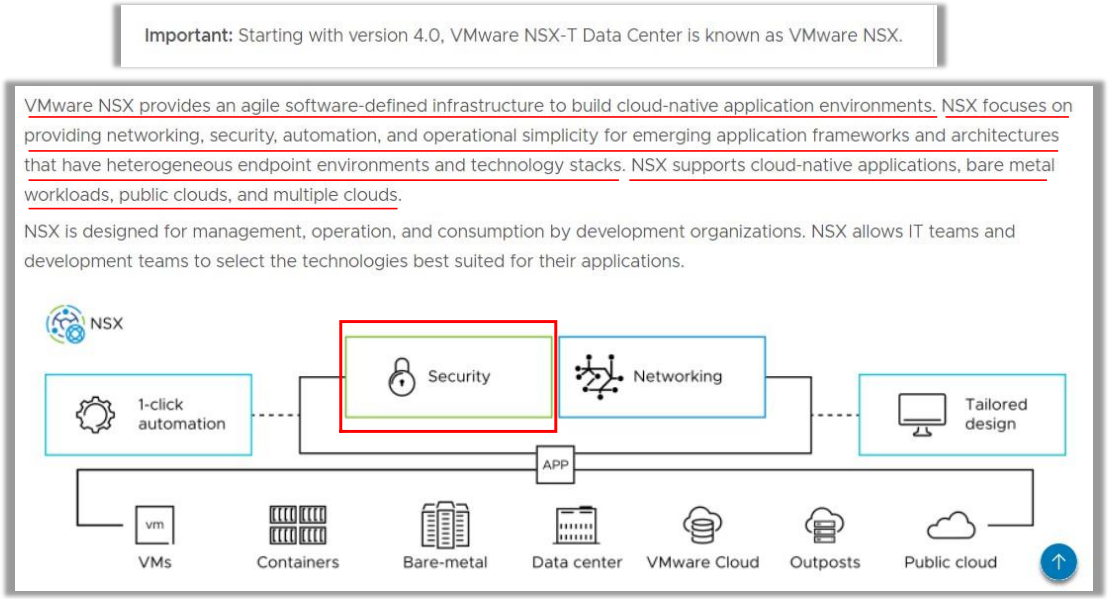
Unless otherwise noted, UMBRA believes and contends that each element of each claim asserted herein is literally met through VMware's provision of the Accused Instrumentalities. However, to the extent that VMware attempts to allege that any asserted claim element is not literally met, UMBRA believes and contends that such elements are met under the doctrine of equivalents. More specifically, in its investigation and analysis of the Accused Instrumentalities, UMBRA did not identify any substantial differences between the elements of the patent claims and the corresponding features of the Accused Instrumentalities, as set forth herein. In each instance, the identified feature of the Accused Instrumentalities performs at least substantially the same function in substantially the same way to achieve substantially the same result as the corresponding claim element.

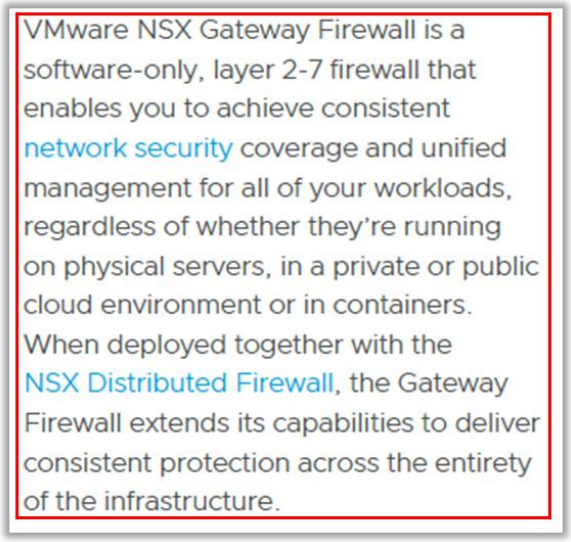
To the extent the chart of an asserted claim relies on evidence about certain specifically identified Accused Instrumentalities, UMBRA asserts that, on information and belief, any similarly functioning instrumentalities also infringes the charted claim. UMBRA reserves the right to amend this infringement analysis based on other products made, used, sold, imported, or offered for sale by VMware. UMBRA also reserves the right to amend this infringement analysis by citing other claims of the '482 patent, not listed in the claim chart, that are infringed by the Accused Instrumentalities. UMBRA further reserves the right to amend this infringement analysis by adding, subtracting, or otherwise modifying content in the "Accused Instrumentalities" column of each chart.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

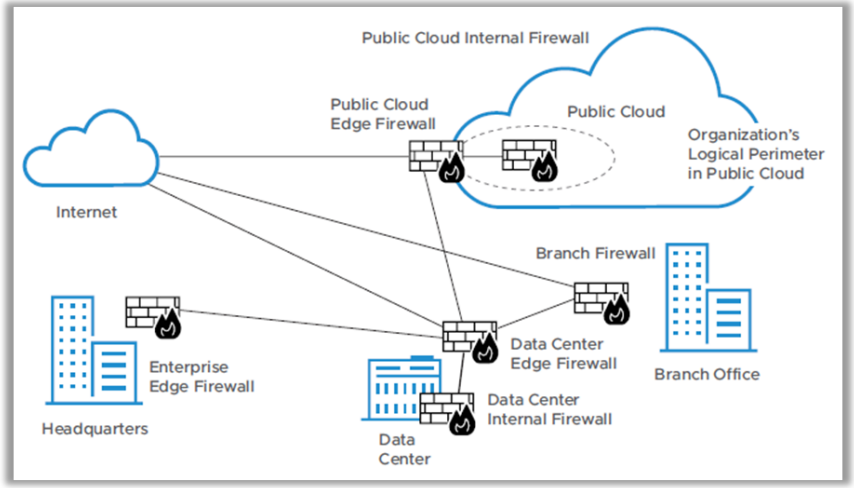
Claim #1	Accused Instrumentalities
Indep.Cl. 1 1-p A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:	"VMware NSX provides an agile software-defined infrastructure to build cloud-native application environments. NSX focuses on providing …, security," i.e., a multi-perimeter firewall system located in a cloud and forming part of a global virtual network.  Source: VMware NSX Documentation, https://docs.vmware.com/en/VMware-NSX/index.html (annotations added) "VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that enables you to achieve consistent network security coverage and unified management for all of your workloads, regardless of whether they're running on physical servers, in a private or public cloud environment or in containers.

1-p Cont.	When deployed together with the NSX Distributed Firewall, the Gateway Firewall extends its capabilities to deliver consistent protection across the entirety of the infrastructure", i.e., a multi-perimeter firewall system located in a cloud and forming part of a global virtual network.  Source: VMware NSX Gateway Firewall data sheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf (annotations added) See also: https://www.vmware.com/products/nsx.html

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

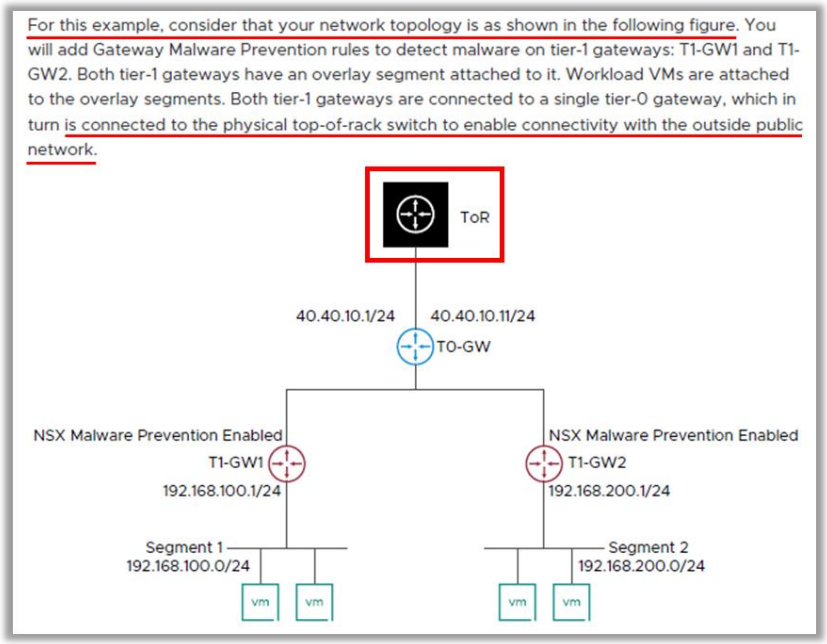
Claims 1-9

1-p Cont.	 Deploying a solution like the VMware NSX Gateway Firewall in conjunction with the NSX Distributed Firewall makes it possible to extend the same unified, consistent access control and threat protection capabilities that the NSX Distributed Firewall supplies across all workloads in the private cloud. And this comprehensive protection can be achieved within a single management console and software-only solution portfolio. This reduces the administrative burden that Source: Protecting Physical Workloads in the Private Cloud white paper, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-protecting-physical-workloads-in-the-private-cloud.pdf_ (annotations added)

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

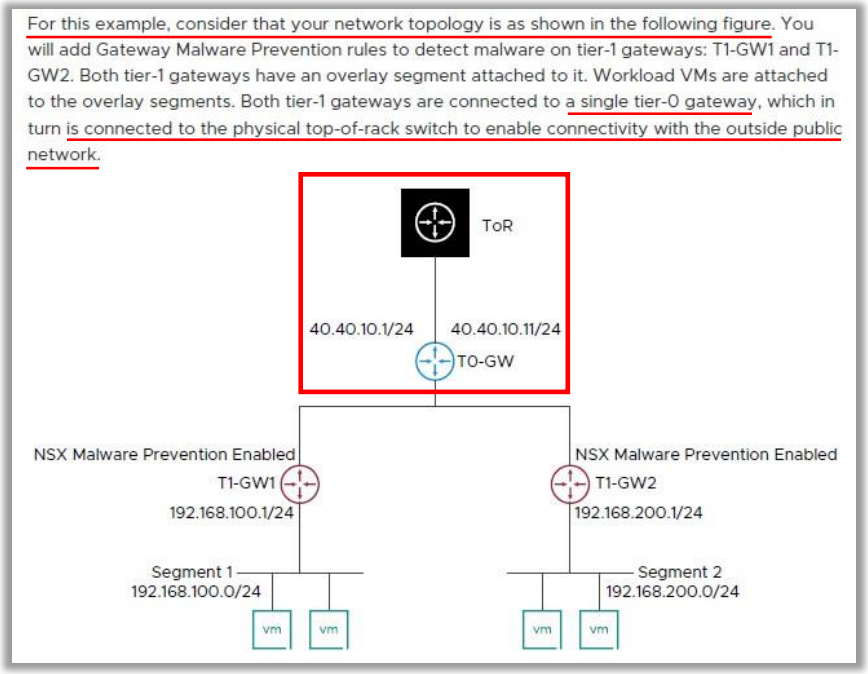
Claims 1-9

1-a an egress ingress point device;	"For this example, consider that your network topology is … is connected to the physical top-of-rack switch to enable connectivity with the outside public network.", i.e., the "top-of-rack switch ToR" is an egress ingress point device.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

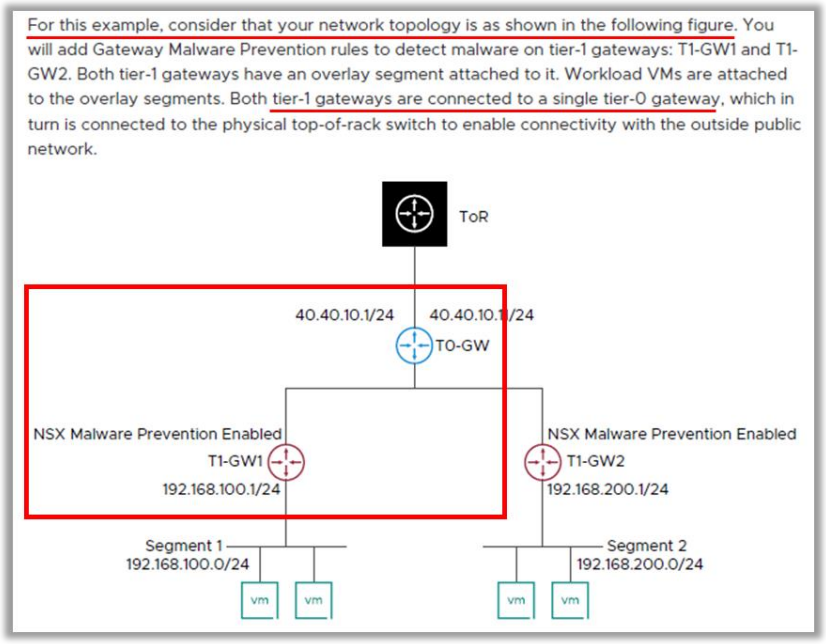
Claims 1-9

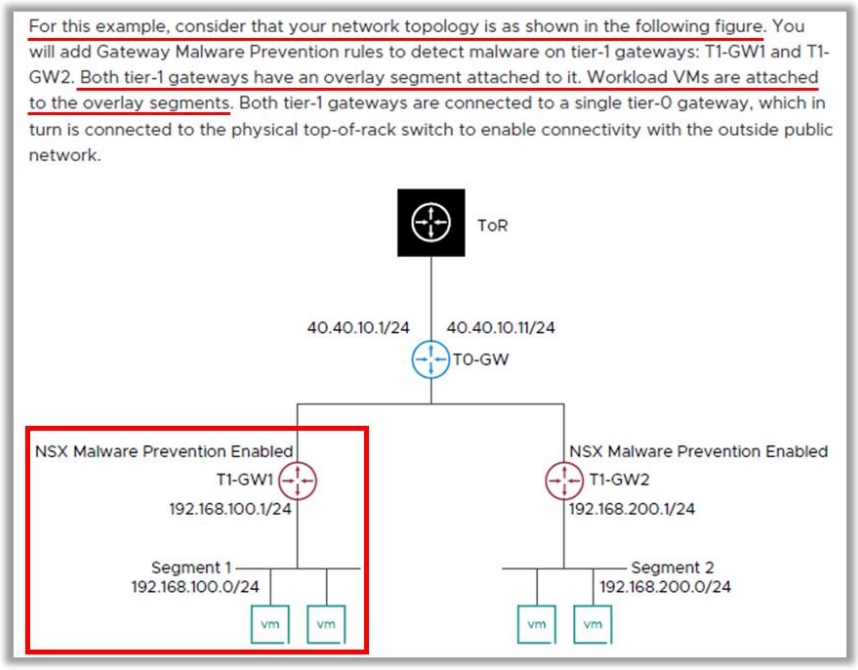
1-b a first access point server in communication with the egress ingress point device;	"For this example, consider that your network topology is as shown in the following figure. … a single tier-0 gateway, … is connected to the physical top-of-rack switch to enable connectivity with the outside public network.", i.e., "a single tier-0 gateway T0-GW" is a first access point server in communication with the "top-of-rack switch ToR" egress ingress point device.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

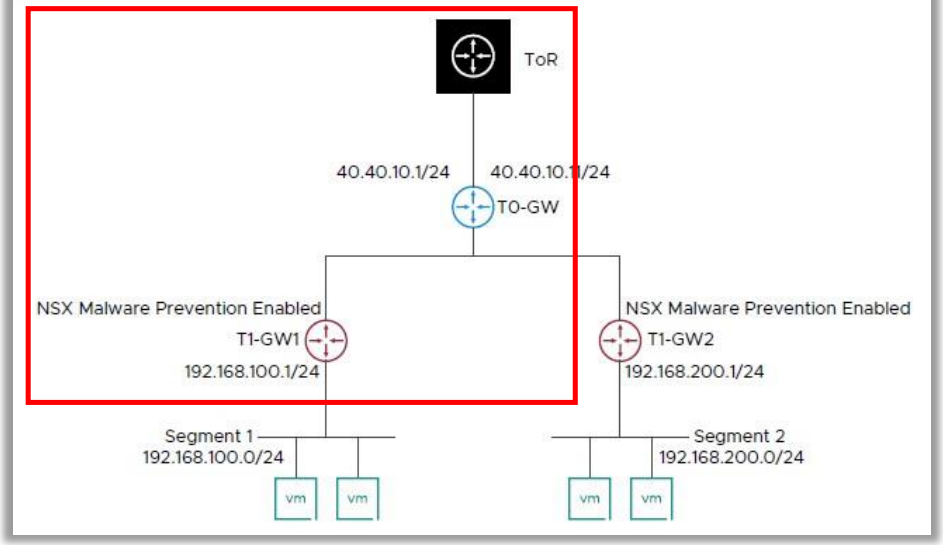
Claims 1-9

1-c a second access point server in communication with the first access point sever;	For this example, consider that your network topology is as shown in the following figure. … tier-1 gateways are connected to a single tier-0 gateway", i.e., "tier-1 gateway T1-GW1" is a second access point server in communication with the "T0-GW tier-0 gateway" first access point server.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

1-d an endpoint device in communication with the second access point server;	"For this example, consider that your network topology is as shown in the following figure. … Both tier-1 gateways have an overlay segment attached to it. Workload VMs are attached to the overlay segments.", i.e., a "Workload VM" is an endpoint device in communication with the "T1-W1 tier-1 gateway" second access point server .  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

1-e a first perimeter firewall in communication with the first access point server,	"VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities … as well as routing … functionality.", i.e., the "VMware NSX Gateway Firewall is software" running on a server that performs first perimeter firewall functions in communication with the "routing" first access point "functionality." VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality. Source: VMware NSX Gateway Firewall data sheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf (annotations added) See also: https://www.vmware.com/products/nsx.html

1-e Cont. wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and	"We can use the NSX-T … Tier-0 Gateway Firewall to provide a stateful rule set to secure traffic between virtual and physical routed or bridged traffic", i.e., the "NSX-T … Tier-0 Gateway Firewall" performs stateful packet inspection to prevent at least some traffic from passing from the "T0-GW" first access point server to the "T1-GW1" second access point server. We can use the NSX-T Tier-1 and Tier-0 Gateway Firewall to provide a stateful rule set to secure traffic between virtual and physical routed or bridged traffic. Source: The NSX-T Gateway Firewall Secures Physical Servers, https://blogs.vmware.com/security/2020/08/the-nsx-t-gateway-firewall-secures-physical-servers.html (annotations added)

1-e Cont.	For this example, consider that your network topology is as shown in the following figure. You will add Gateway Malware Prevention rules to detect malware on tier-1 gateways: T1-GW1 and T1-GW2. Both tier-1 gateways have an overlay segment attached to it. Workload VMs are attached to the overlay segments. Both tier-1 gateways are connected to a single tier-0 gateway, which in turn is connected to the physical top-of-rack switch to enable connectivity with the outside public network.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

1-f a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,	"VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities … as well as routing … functionality.", i.e., the "VMware NSX Gateway Firewall is software" running on a server that performs second perimeter firewall functions in communication with the "routing" second access point "functionality." VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality. Source: VMware NSX Gateway Firewall data sheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf (annotations added) NOTE: Malware is typically part of DPI. URL filtering and IDS/IPS is typically part of SPI. See also: https://www.vmware.com/products/nsx.html

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

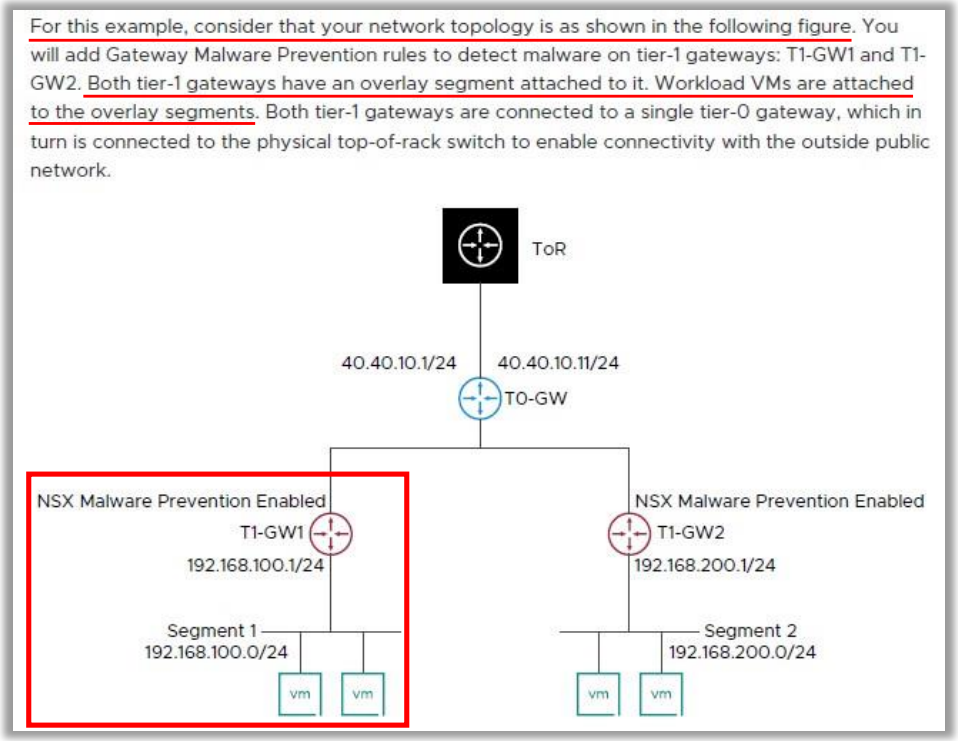
Claims 1-9

1-f Cont.	"VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection." "The objective of NSX Intrusion Detection and Prevention Service (IDS/IPS) is to monitor network traffic", i.e., perform deep packet inspection "on the hosts and edges for malicious activity by comparing the traffic against a known set of signatures. The objective of NSX Malware Prevention is to extract files from the network traffic on the hosts and edges and analyze these files for malicious behavior" to prevent at least some traffic from passing from the "T1-GW1" second access point server to the "Workload VM"end point device. "NSX IDS/IPS for a Gateway Firewall is supported only for tier-1 gateways." VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality. Source: VMware NSX Gateway Firewall data sheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf (annotations added) The objective of NSX Intrusion Detection and Prevention Service (IDS/IPS) is to monitor network traffic on the hosts and edges for malicious activity by comparing the traffic against a known set of signatures. The objective of NSX Malware Prevention is to extract files from the network traffic on the hosts and edges and analyze these files for malicious behavior. Source: NSX-T Data Center Administration Guide, p. 454 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

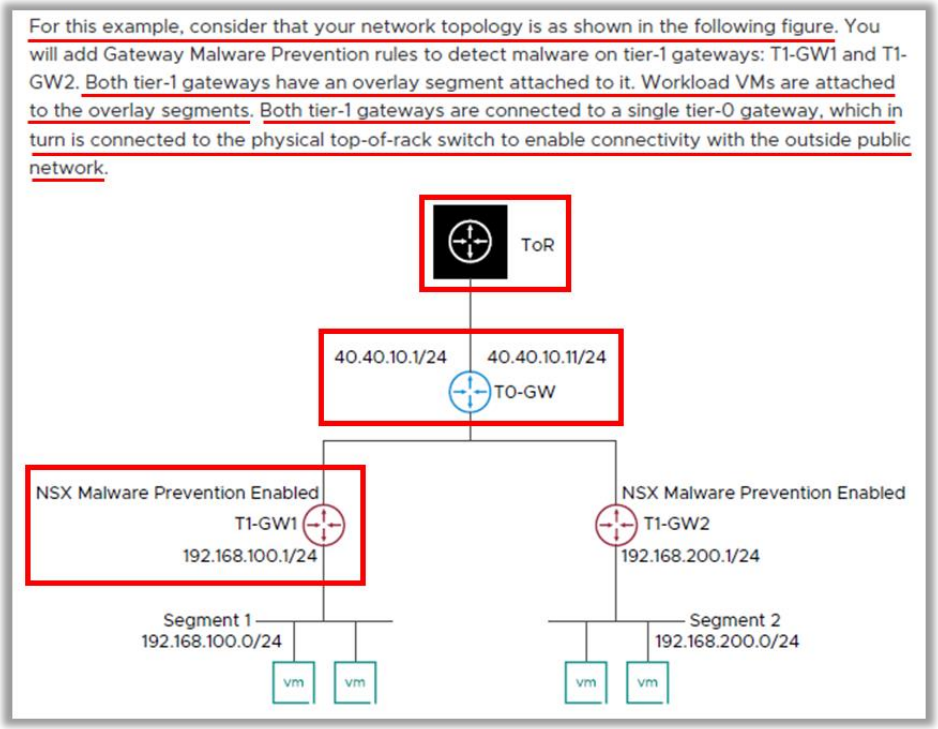
UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

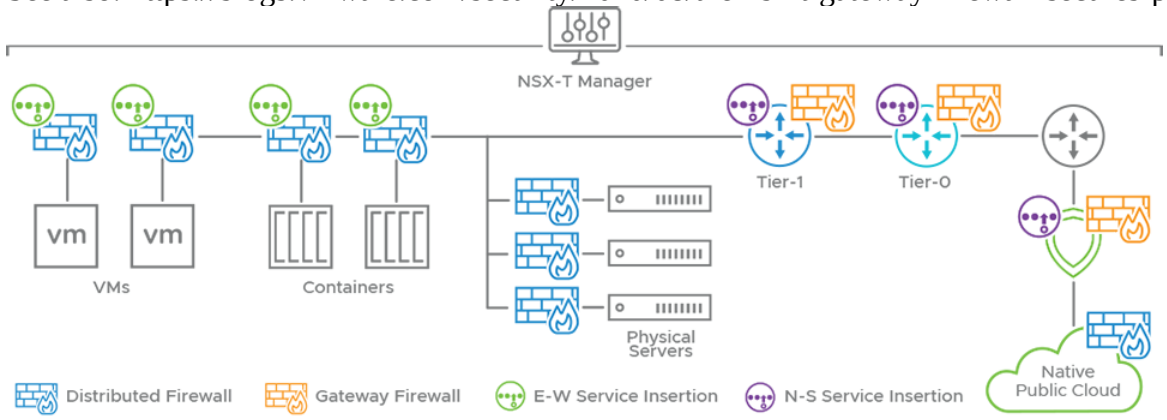
U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

1-f Cont.	 Source: NSX-T Data Center Administration Guide, p. 501 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

1-f Cont. wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,	The NSX Gateway Firewall, which is a software based layer 2-7 firewall and is instantiated on the Tier-1 gateway ("second perimeter firewall"), is the "second perimeter firewall". The "Top-of-Rack switch", i.e., egress ingress point device is a physical device, and it comprises hardware. Additionally, the NSX gateway firewalls on both the "T0-GW tier-0 gateway" and "T1-GW1 tier-1 gateway" access point servers run on hardware, e.g., Intel Xeon. The table below summarizes the performance characteristics of the NSX Gateway Firewall under different resource envelopes. Form Factor / Large (8 vCPU, 16GB RAM) / X-Large (16 vCPU, 64GB RAM Firewall throughput (64 KB HTTP): 20 Gbps / 24 Gbps IPsec VPN throughput: 13 Gbps / 21 Gbps IDS/IPS (64 KB HTTP): 1.5 Gbps / 4.5 Gbps Malware detection (64 KB HTTP): Not supported / 3.5 Gbps New sessions per second: 306 K / 310 K Max sessions: 2.1 million / 4.2 million The performance results shown above were tested under the following conditions: • Firewall and IPsec VPN throughput measured with Intel® Xeon® CPU E5-2660 v4 2.00GHz with 40G port network interface card. Source: VMware NSX Gateway Firewall data sheet, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf (annotations added)

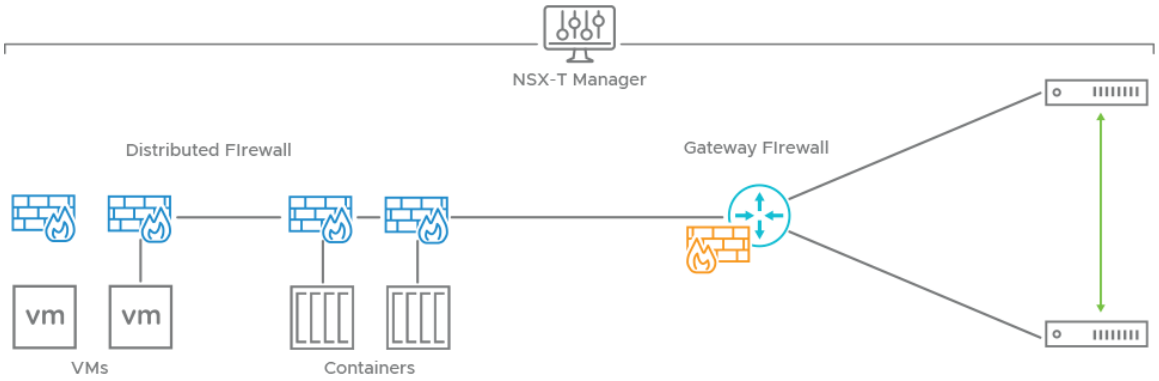
1-f Cont.	For this example, consider that your network topology is as shown in the following figure. You will add Gateway Malware Prevention rules to detect malware on tier-1 gateways: T1-GW1 and T1-GW2. Both tier-1 gateways have an overlay segment attached to it. Workload VMs are attached to the overlay segments. Both tier-1 gateways are connected to a single tier-0 gateway, which in turn is connected to the physical top-of-rack switch to enable connectivity with the outside public network.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

1-f Cont.	See also: https://blogs.vmware.com/security/2020/08/the-nsx-t-gateway-firewall-secures-physical-servers.html  We can use the NSX-T Distributed Firewall to provide a stateful firewall policy for traffic ingressing or egressing to any virtual workload, or **any physical workload using NSX-T bare metal agents in any site, and any cloud.** Source: https://blogs.vmware.com/security/files/2020/07/Graphic-2.png

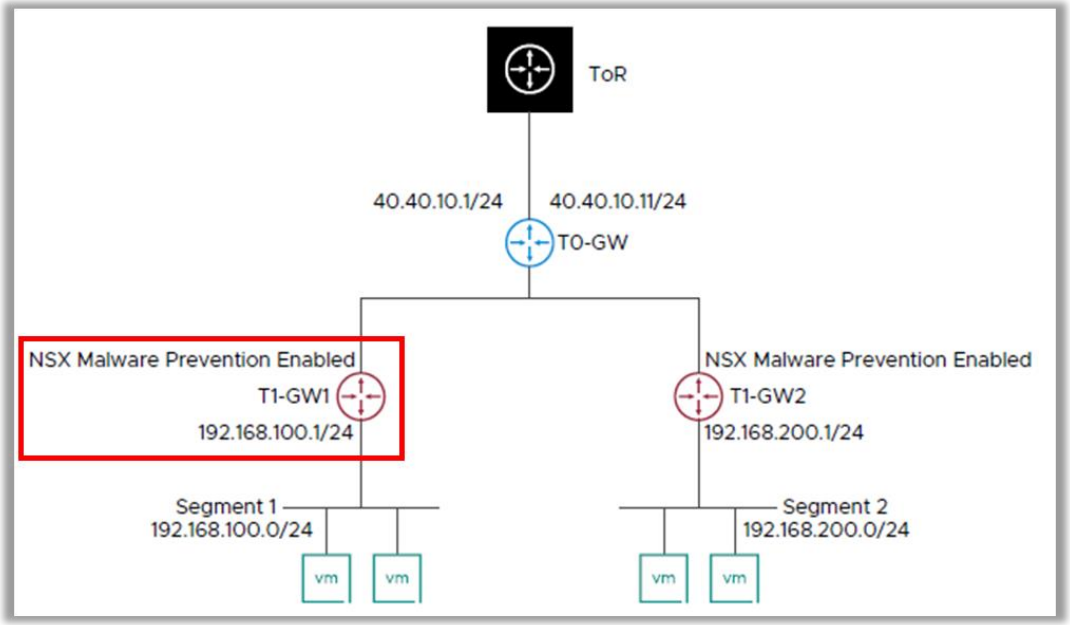
UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

1-f Cont.	See also:  https://blogs.vmware.com/security/files/2020/07/Graphic-5.png This last use case, physical to physical server security, involves selection of either stateless or stateful firewall rules depending upon the routing design or use of service interfaces. In most cases, a stateful firewall design is possible. "In this example, your objective is to create security policies with Gateway Firewall rules that detect malicious files on the north-south traffic, which is passing through the NSX Edges in your NSX-T Data Center." "A Malware Prevention profile named Profile_T1-GW is added with the following configuration: All file category options are selected. Cloud File Analysis option is selected." NOTE: "Cloud File Analysis" also supports "cloned" copies.

1-f Cont. wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.	"File events are generated when files are extracted by the IDS engine on the NSX Edges in the north-south traffic and by the NSX Guest Introspection agent on the virtual machine endpoints in the distributed east-west traffic. NSX Malware Prevention feature inspects the extracted files to determine whether they are benign, malicious, or suspicious." This example demonstrated that the "T1-GW1 tier 1 gateway" second perimeter firewall performs deep packet inspection to generate file event extract file, i.e., cloned copy of traffic that flows through the second perimeter firewall for inspection per the selected Cloud File Analysis option.,

1-f Cont.	Example: Add Rules for NSX Malware Prevention on a Gateway Firewall In this example, your objective is to create security policies with Gateway Firewall rules that detect malicious files on the north-south traffic, which is passing through the NSX Edges in your NSX-T Data Center.  Source: NSX-T Data Center Administration Guide, p. 506 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

1-f Cont.

- A Malware Prevention profile named `Profile_T1-GW` is added with the following configuration:
  - All file category options are selected.
  - **Cloud File Analysis** option is selected.

  You will use this Malware Prevention profile in the Gateway Firewall rules of both tier-1 gateways.

Name	ID	Sources	Destinations	Services	Security Profiles	Applied To	Mode
N_to_S	1011	North	South	HTTP	Profile_T1-GW	T1-GW1	Detect Only
S_to_N	1010	South	North	HTTP	Profile_T1-GW	T1-GW1	Detect Only

Source: NSX-T Data Center Administration Guide, p. 507 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

Monitoring File Events

File events are generated when files are extracted by the IDS engine on the NSX Edges in the north-south traffic and by the NSX Guest Introspection agent on the virtual machine endpoints in the distributed east-west traffic.

NSX Malware Prevention feature inspects the extracted files to determine whether they are benign, malicious, or suspicious. Each unique inspection of a file is counted as a single file event in

Source: NSX-T Data Center Administration Guide, p. 511 https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsxt_32_admin.pdf (annotations added)

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

See also: Image Clipped from PDF file: vmw-nsx-sandbox-solution.pdf - on page 1 (top right)

Network Sandbox

At a Glance

VMware's Network Sandbox provides advanced malware analysis of artifacts traversing your cloud environment. The sandbox deconstructs every behavior engineered into a file or URL and sees all instructions that a program executes, all memory content, and all operating system activity.

At VMware, Network Sandboxing is a component of NSX Advanced Threat Prevention along with Intrusion Detection/Prevention System (IDS/IPS), Network Traffic Analysis (NTA), and Network Detection and Response (NDR).

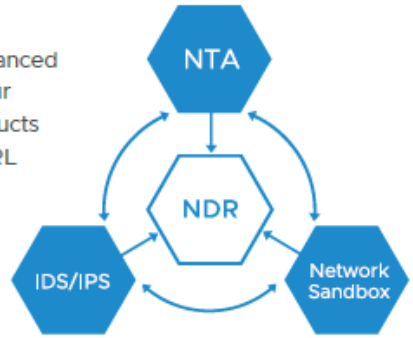
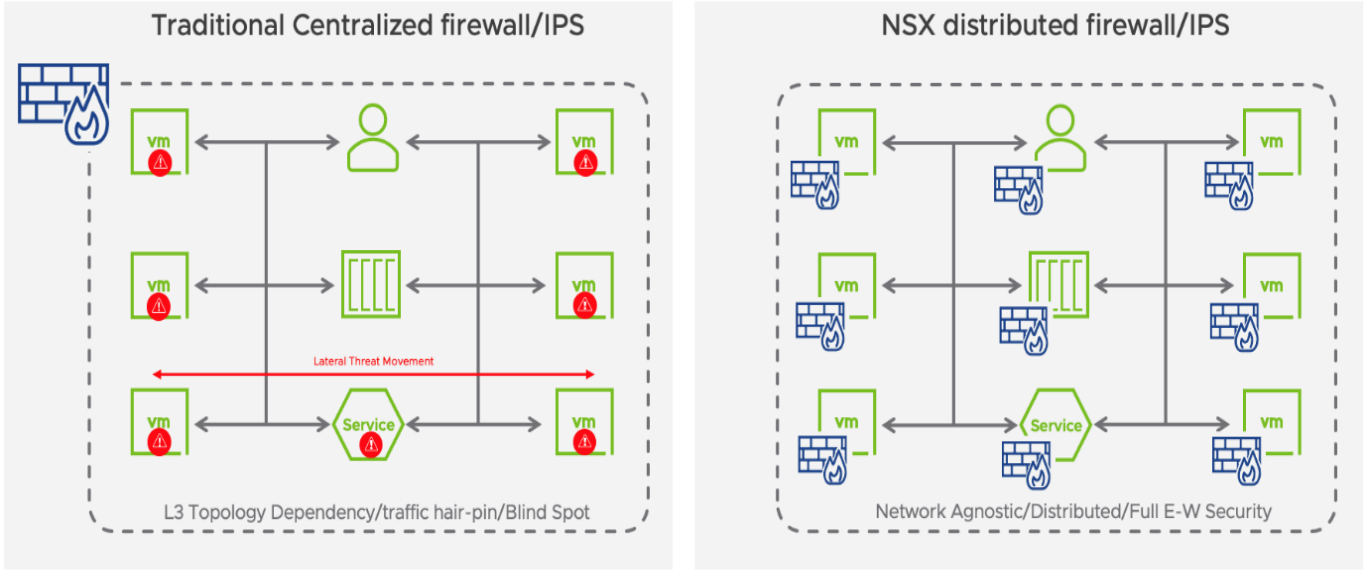


Figure 1: NSX Advanced Threat Prevention = IDS/IPS + Network Sandbox + NTA + NDR

The Network Sandbox operates and analyzes behavior based on a cloned copy.

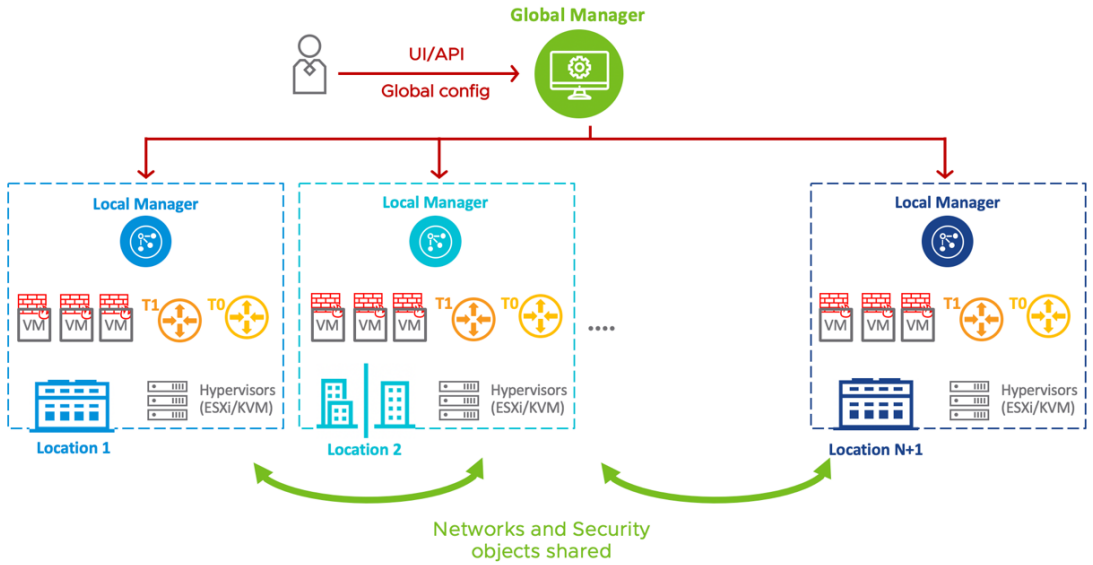
Source: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-sandbox-solution.pdf

Claim #2	Accused Instrumentalities
2. The multi-perimeter firewall system according to claim 1, wherein at least one of the access point servers is configured to perform firewall services.	See: https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-13-datacenter-security-layoutchallengessolution  Figure 1-3: Traditional Appliance Firewall vs NSX distributed firewall Source: https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.005.png

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

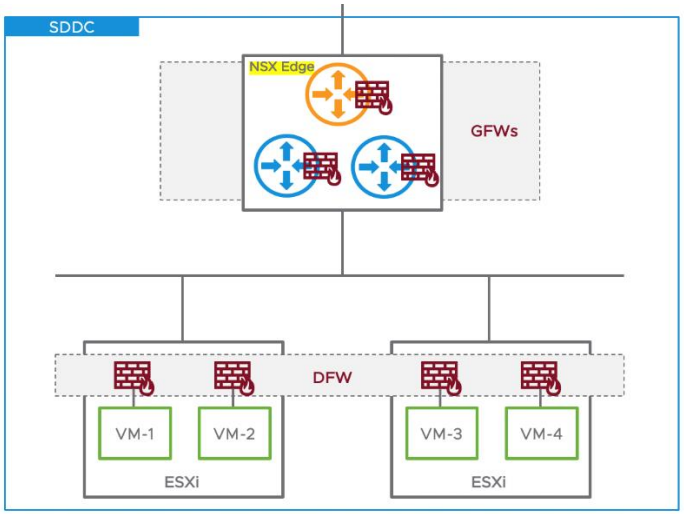
Claims 1-9

Claim #3	Accused Instrumentalities
3. The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.	See https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-9-federation  Figure 9 - 2 NSX-T Federation https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.117.png

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

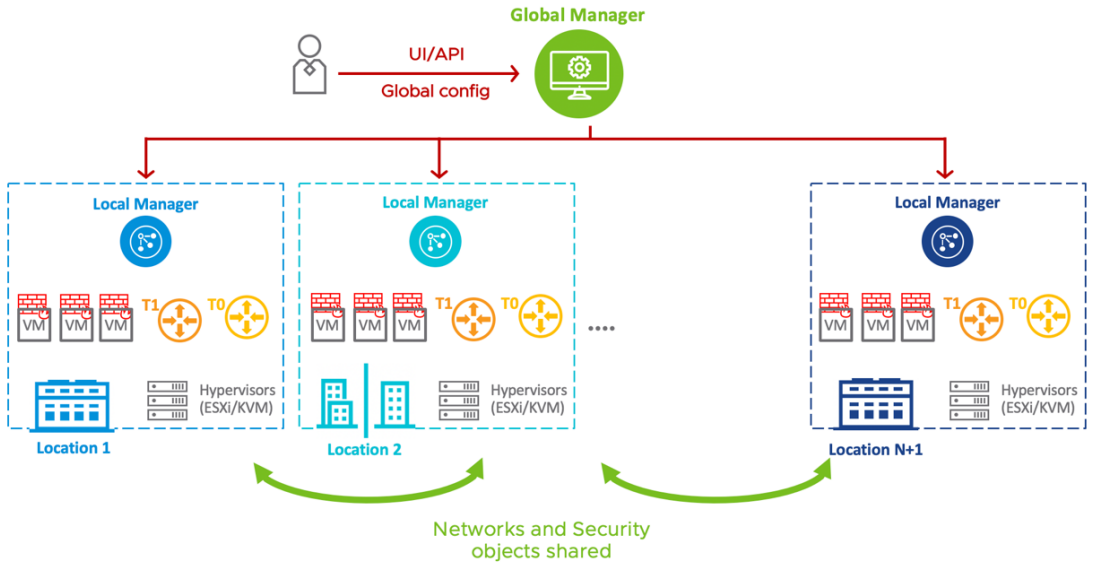
Claims 1-9

Claim #4	Accused Instrumentalities
4. The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a network path.	See https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-41-nsx-firewalling-a-new-approach  Figure 4 - 1 NSX-T Firewalls https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.029.png

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

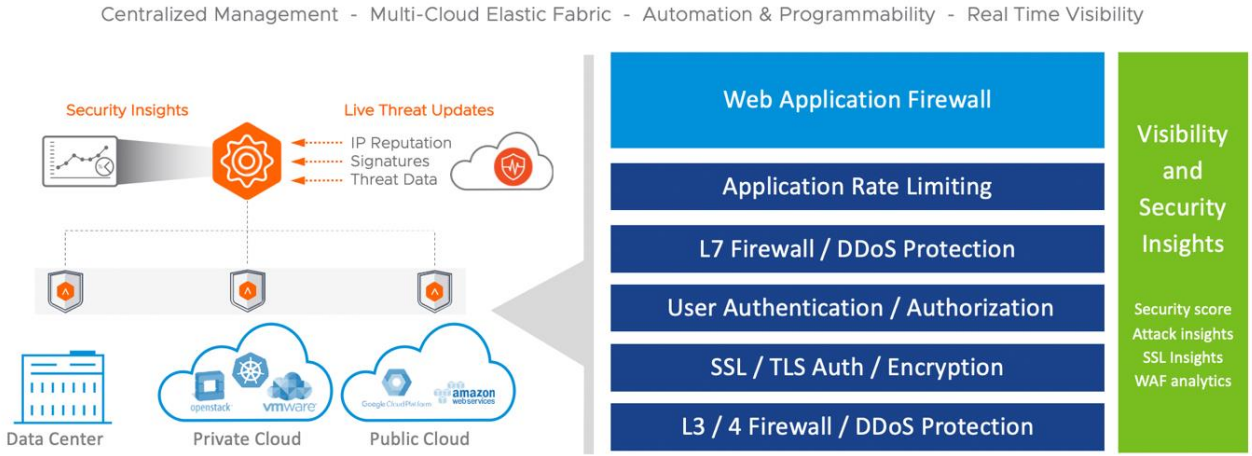
Claims 1-9

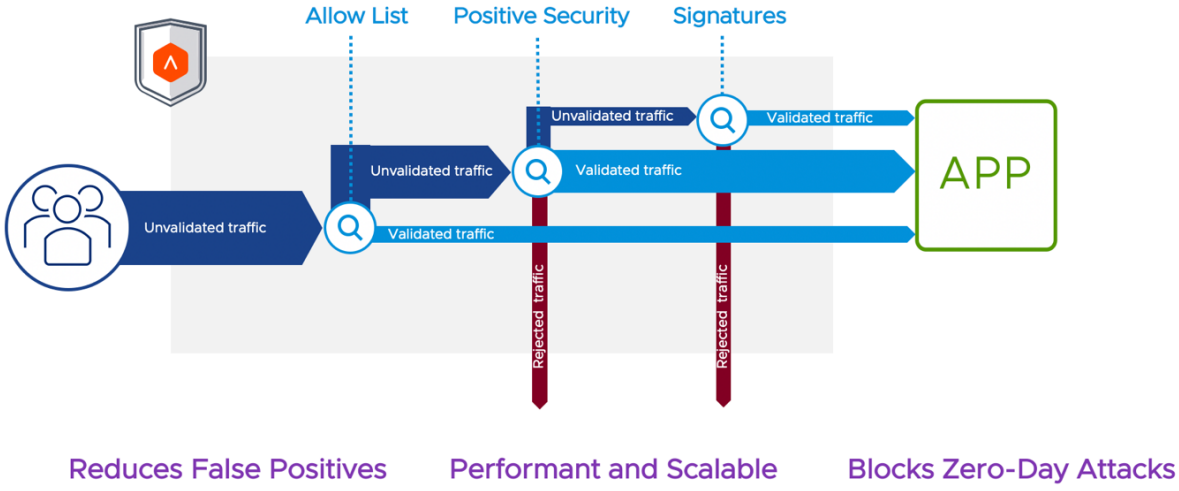
Claim #5	Accused Instrumentalities
5. The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a network back channel.	See https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-9-federation  Figure 9 - 2 NSX-T Federation https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.117.png

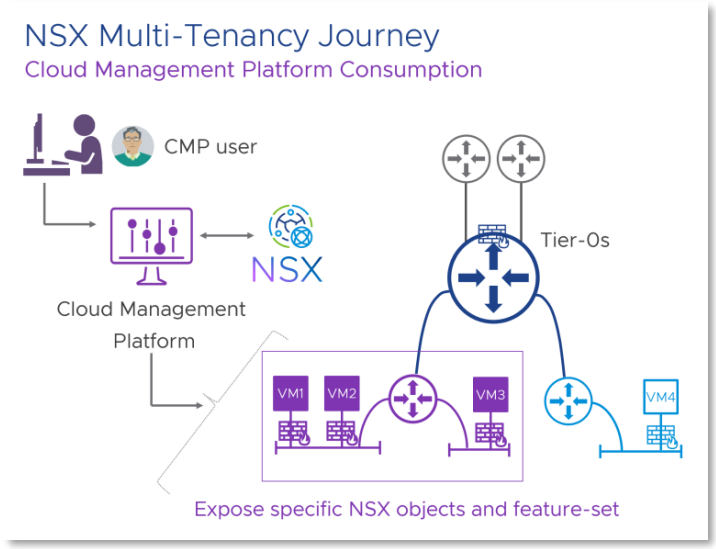
UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

Claim #6	Accused Instrumentalities
6. The multi-perimeter firewall system according to claim 3, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.	See https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-42--gateway-firewall  Figure 4 - 7 Advanced Load Balancer Security Service Suite

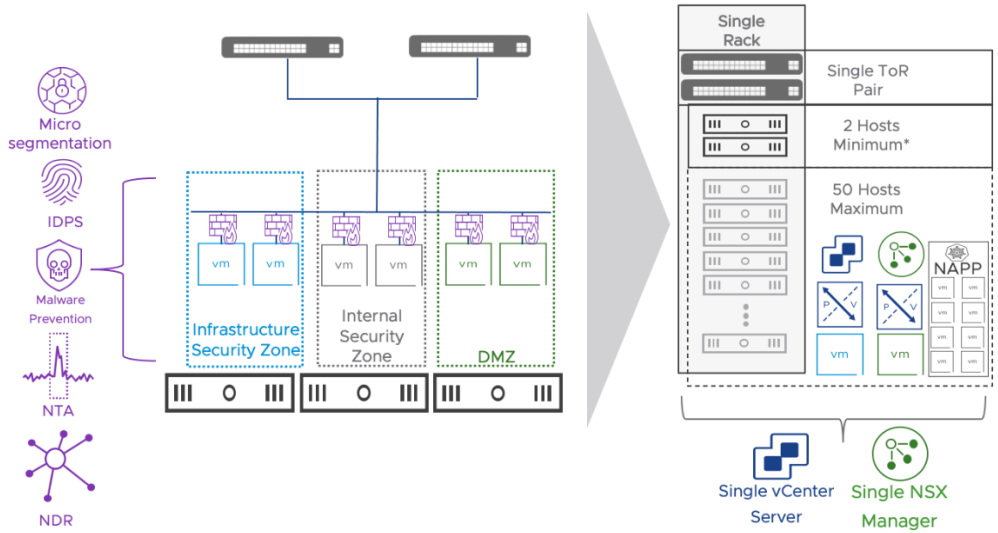
Clm. 6 Cont.	See also:  Figure 4 - 8 WAF Security Pipeline https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.036.png Also see claim 9 below regarding "scalable" aspect of the pipeline.

Claim #7	Accused Instrumentalities
7. The multi-perimeter firewall system according to claim 6, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.	See: https://blogs.vmware.com/networkvirtualization/2023/03/nsx-multi-tenancy.html/  https://blogs.vmware.com/networkvirtualization/files/2023/03/multi-blog-5-768x586.png The model shown below allows a provider to set up the Tier-0 Gateway, define how it connects to the network, and expose the creation of Tier-1s through a Cloud Management Platform (such as Aria Automation, OpenStack or vCloud Director). Tenancy is achieved from a data-plane perspective through NSX and from a management plane perspective through a Cloud Management Platform, which isolates the different environment configurations.

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

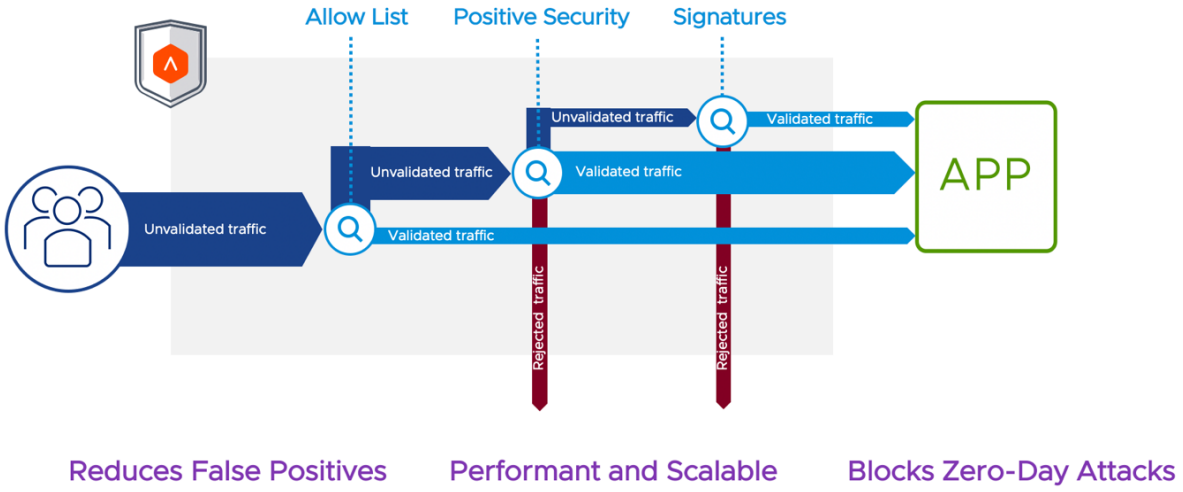
U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

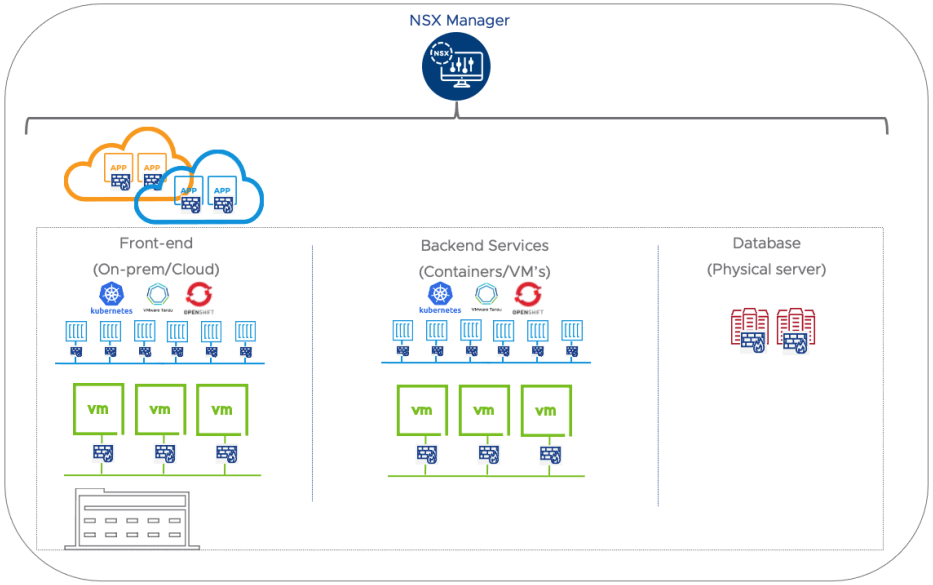
Claims 1-9

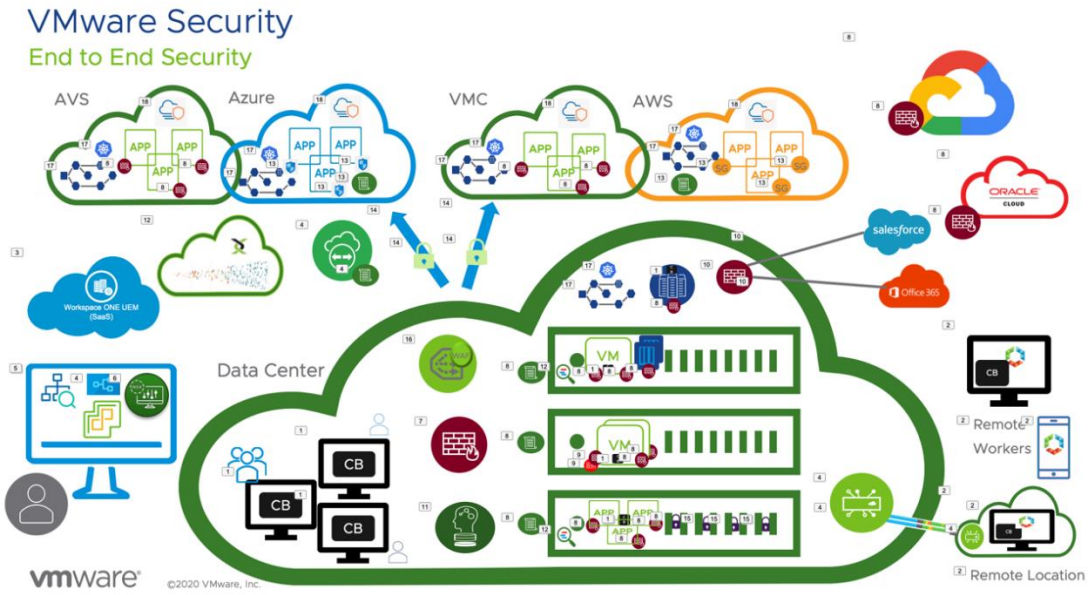
Claim #8	Accused Instrumentalities
8. The multi-perimeter firewall system according to claim 1, wherein the deep packet inspection is performed on flow through traffic.	See: https://nsx.techzone.vmware.com/resource/nsx-easy-adoption-design-guide#a-23-simple-security-for-applications-overview  Figure 9: Simple Security Use Case Architecture and Features when the NSX Application Platform (NAPP) is deployed https://images.nsx.techzone.vmware.com/sites/default/files/imported-images/node_2684_1216-105346/9016-1216-105338/9016-1216-105338-12.png

 Note: All internet sources last accessed and downloaded July 31, 2023.

Claim #9	Accused Instrumentalities
9. The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.	See: https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-21-nsx-security-use-cases **2.1.7.3 How to take a journey with NSX** NSX helps in having consistent policy across the virtual machine, container, Physical server, and cloud instances. NSX allows an organization to have a zero-trust model even for distributed multi-tier applications across different environments and/or different form factor. For example, a multi-tier application can have its front-end deployed on multiple clouds and/or on-prem for high availability and business continuity. The back-end services could be hosted on on-prem as a virtualized service, or containerized micro-service and back-end databases are hosted on a physical server. This type of multi-cloud, multi-form factor distributed application can be protected using NSX micro-segmentation policy to have the zero-trust model. See also claim 6 regarding figure below.

Clm. 9 Cont.	See also:  Figure 4 - 8 WAF Security Pipeline https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.036.png NOTE: The scalable aspect of the security pipeline implies load balancing and allocation of resources on demand.

Clm. 9 Cont.	See also:  https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.013.png Figure 2-8: Consistent policy across diverse workloads See also: https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-104--nsx-operations

Clm. 9 Cont.	 Figure 1- 1 VMware Security Offering https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.133.png

UMBRA TECHNOLOGIES LTD.'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 10,574,482– Defendant VMware Inc. - UMBRA Technologies Ltd. ("UMBRA")

Claims 1-9

Clm. 9 Cont.	Also see: https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.133.png "**1 – VMware Carbon Black** – CB allows customers to detect and stop threats with endpoint and workload security. **2- VMware Horizon View** - Horizon allows for the secure delivery of virtual desktop infrastructure. **3 – WorkspaceONE –** WorkspaceONE is a Unified Endpoint Manager (UEM) which provides a single point of definition and control of the intersection of application/user/device/location. **4 – VMware SD-WAN by VeloCloud** – Traffic to remote locations can be secured (and optimized through DMPO – Dynamic MultiPath Optimization) using SD-WAN by VeloCloud. Now, with Secure Access Service Edge (SASE) functionality, the admin can also define secure connectivity policy. **5– vRealize Network Insight** - vRNI provides visibility into the physical underlying infrastructure of switches and routers as well as the virtual infrastructure through netflow, or into the legacy firewall infrastructure through integration with a variety of firewall managers. This visibility is complemented by a cross sectional view of the virtual infrastructure from native Amazon Web Services (AWS) and Microsoft Azure environments to branches to ESXi VMs and Kubernetes (K8) containers. This ubiquitous view combines into a complete picture of the environment which is searchable. In addition, an admin can get firewall policy suggestions or just determine the path with applicable security policies along every step from point A to point B. **6 – NSX-T Data Center** – This document will focus on the security features of NSX. To provide context in the greater picture, items 7 through 14 provide a listing of the security components of NSX. **7 –NSX Gateway Firewall –** NSX Gateway Firewall secures the data center boundary. It also provides security at the physical to virtual boundary as well as tenant boundaries, in multi-tenant environments.

Clm. 9 Cont.	**8 – NSX Distributed Firewall** - For East-West security, the admin can centrally define policy from the NSX Manager. NSX leverages a distributed local control plane to implement policy definition using local constructs (be they firewall rules on every virtual NIC (vnic) of a VM or agents running on physical servers). NSX Distributed Firewall runs on ESXi or KVM hypervisors, on prem or in several clouds. It also runs as part of the NSX Container Plug-in (NCP) which supports K8, RedHat OpenShift, and Tanzu container platforms. **9 – NSX Identity Firewall** – NSX IDFW uses Active Directory User SIDs to provide user-context for single-user Horizon/Citrix VDI and server OS cases, and server OS use cases, as well as multi-user, RDSH use cases such as Horizon Apps and Citrix Published Applications/Virtual Apps. **10 – NSX URL Filtering –** NSX also provides URL filtering capabilities, whether it is to ensure that malicious websites are not being accessed (such as by ransomware for Command and Control) or by users misguided sense of where to download software. **11 – NSX Intelligence** – NSX Intelligence is a native distributed analytics platform, that leverages workload and network context from NSX, to deliver converged security policy management, analytics, and compliance. **12 – NSX Advanced Threat Prevention (ATP)** – From the Lastline acquisition, ATP delivers network traffic analysis and advanced malware analysis with comprehensive network detection and response capabilities. **13 – NSX IPS** - For intrusion detection, NSX brings industry first distributed IPS (Intrusion Detection and Prevention System). This not only provides distributed, scalable IPS but also prevents misfires through unparalleled context. **14 - NSX Cloud** – For AWS and Azure native workloads, NSX Cloud offers a single point of policy control across VPCs and VNETs to ensure policy consistency. For AWS and Azure native environments, security can be implemented either via agents on workloads or natively via cloud controls

	15 – IPSec VPN – To access cloud environments (such as for direct connect) or anywhere else, NSX ensures the in flight traffic is encrypted using IPSec VPN. **16 – vSAN Disk Encryption** –For data at rest, vSAN disk encryption ensures data is safe. **17– Web Application Firewall** – NSX provides integrated load balancing. With our Advanced LB, comes iWAF: intelligent WAF that uses analytics and machine learning to tune policy and insights into attack traffic. **18 - Tanzu Service Mesh** – For the security of microservice applications across K8 clusters and clouds, VMware provides Tanzu's service mesh. **19 – Secure State -** Finally, VMware Secure State correlates risk across this dynamic cloud infrastructure, reporting on risk such as "any any allow" configuration changes. This vast offering of products and features allows for pervasive and granular security policy definition from endpoints to servers to containers to microservices. It also allows for encrypting data both in flight and at rest. Finally, this also allows for the detection of suspicious behaviors on endpoints or in the network across a heterogeneous environment." Source: https://nsx.techzone.vmware.com/sites/default/files/imported-images/node_2490_0616-165419/NSX%20Security%20Reference%20Guide/NSX%20Security%20Reference%20Guide.133.png

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same.